WHITE PAPER

Version 1.0 | **FEB 2018**

Echo® 21CFR11 Compliance Manager (ECM) Software Provides Comprehensive Title 21 CFR Part 11 Compliance Features

YOUR CHALLENGE

FDA's "Part 11" Electronic Records Electronic Signatures combined with CDER's Guidance for Industry Computerized Systems Used in Clinical Investigations (May 2007) define the requirements for creation, maintenance, storage, and modification of electronic records, submitting documentation to FDA in electronic form, use of electronic signatures, as well as the infrastructure a company must maintain to demonstrate compliance. These regulations and guidelines add challenges to the regulated life science industries. The FDA now often requests raw data sets and wants to be able to use the same tools that you used to evaluate data. Compliance inspectors will look for the required infrastructure. The FDA requires that the original data set be kept intact and that all changes to the data are identified including what was changed, who changed it, and the date of the change. This allows FDA to review all the details about how you arrived at your conclusions.

THE SOLUTION

Echo® 21CFR11 Compliance Manager (ECM) software with Title 21 CFR Part 11 Compliance is designed to limit access for creation and maintenance of electronic records, maintains a permanent record of changes to data and reports, and allows archiving and retrieval of data. ECM works seamlessly with your Echo Software Applications and Echo Liquid Handlers to provide you the tools that enable you to be Part 11 compliant. ECM software has the following features to integrate with your Part 11 compliance program:

- **Security, Access Limitations, and Authority Checks** allows you to control which functions people can perform on a user-based level and records the name and date of the person making changes to the data. Three levels of security permissions can be set for each security group.
- **Record Protection** prevents unauthorized manipulation of ECM software produced datasets and reports. Raw data can be stored with metadata and reports, facilitating protection and traceability.
- **Audit Trails:** ECM software employs secure, computer-generated, time-stamped audit trails to track actions that create, or modify layout files and reports.
- **Electronic Signatures:** When users are satisfied with their analysis, they can electronically sign it. Signing events are maintained in the audit trail. Signed reports can be securely transferred in a variety of formats within your laboratory information management system.
- **Part 11 Compliance Validation Package:** Labcyte has developed a suite of procedure templates and forms as required by the Guidance for Industry Computerized Systems Used in Clinical Investigations to assist you in validation of the software and integration of the use of electronic records and signatures into your quality system.
- **Much, much more:** sophisticated encryption, print logging, print tagging, password aging and many other features serve to help you ensure that your analysis is in full compliance with Part 11 regulations.
- **New security features that have been added to ECM software.**

Our 21 CFR Part 11 Compliance Matrix highlights all the Part 11 regulations and how ECM software facilitates your compliance with them.

LABCYTE™

CONTACT INFO:

Russell Burge
rburge@labcyte.com

- It is important to ensure that your data meet the highest standards of traceability, reproducibility, and accuracy.

ECM Software now with 21 CFR Part 11 Compliance Support meets those needs

Subpart	Summary of Requirement	Meets Req.	Compliance Strategy
11.10	Control for Closed Systems	Yes	ECM software is designed to run as a closed system: it can only be accessed via the ECM software user interface. Permissions to access ECM software must be granted in Active Directory.
11.10 (a)	Validation	Yes	Labcyte has validated ECM software and developed documentation templates to assist you with validating the software to meet your requirements.
11.10 (b)	Record Generation and Copying	Yes	ECM software stores its report files and results in either human readable PDF or CSV formats or Labcyte proprietary machine-readable formats. CSV formats are not Part 11 compliant formats.
11.10 (c)	Record Protection	Yes	Records are saved in an encrypted format, with checksum measures in place to detect tampering. Original data files are created as write once read many files to prevent changing original data. Labcyte advises that you export your ECM files and save them in a secure folder that has been protected by your disaster recovery system. Labcyte can provide procedure templates for implementing these activities.
11.10 (d)	Access Limitations	Yes	ECM software contains security features that limit access to authorized individuals.
11.10 (e)	Audit Trails	Yes	ECM complies with audit trail requirements to ensure that only authorized additions, deletions, or alterations of information in the electronic record occur. ECM also provides a means to reconstruct details about study conduct and verify the quality and integrity of data.
11.10 (f)	Operational System Checks	N/A	This does not apply to ECM software.
11.10 (g)	Authority Checks	Yes	User access permission is required to access ECM software.
11.10 (h)	Device/Terminal Checks	Yes	ECM software applies checks to assure it has received a valid flow of all analysis data.
11.10 (i and j)	Training and User Accountability	C.S.*	Labcyte can assist your laboratory with preparation of a training plan so that your scientists understand how to use ECM software as well as the implications of Part 11 on their work.
11.10 (k)	System Document Control	Yes	Labcyte follows change control and software life cycle management procedures for document control.
11.30	Controls for Open Systems	N/A	This does not apply to ECM software. ECM software is a Closed System.
11.50 (a)	Identification and Meaning of Electronic Signatures	Yes	ECM software maintains an audit trail of important changes to protocols, ECM software captures electronic signatures of data files or analyses to indicate review, approval, responsibility or authorship. Once data have been produced in a pdf file, these meanings can be enacted.
11.50 (b)	Security and Display of Electronic Figures	N/A	ECM software does not support electronic signatures of data files or analyses to indicate review, approval, responsibility or authorship. Once data has been produced in a pdf file, these meanings can be enacted.
11.100 (a), 11.200 (b)	Uniqueness of Electronic Figures	Yes	ECM software assures that all user ID's are unique, therefore all electronic signatures are unique.
11.100 (b)	Verification of Identity	Yes	You must verify the identity of your ECM software User.
11.100 (c)	Certification	C.S.*	You must certify with FDA that you intend to use electronic signatures.
11.200 (a)(1)	Two-Component Signing	Yes	ECM software requires user security rights to access the software and user name and password to save analysis data and sign Part 11 compliant reports and printouts.
11.200 (a)(2), and (a)(3)	Signature Authenticity and Collaboration to Falsify	C.S.*	To gain access to ECM software, to save analysis data and to sign Part 11 compliant reports and printouts, users must have a valid user name and password.
11.200 (b)	Biometric Signatures	N/A	Not required for ECM software since it operates as a Closed System.
11.300 (a)	Unique Username/Password combinations	C.S.*	
11.300 (b)	Password Aging	Yes	ECM software uses Active Directory to manage password aging.
11.300 (d)	Controls to Prevent Unauthorized Credential Use	Yes	Using Active Directory, ECM software installations can disable accounts after a configurable number of failed logon attempts.
11.300 (e)	Password Testing	C.S.*	

* C.S.: Customer Supplied